




# 2021长安“战疫”网络安全卫士守护赛 misc部分writeup

原创

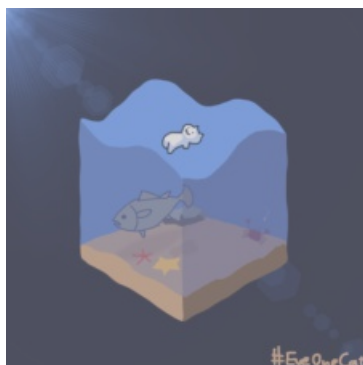
shu天  于 2022-01-13 19:45:58 发布  113  收藏

分类专栏: [# misc ctf](#) 文章标签: [ctf misc](#)

不允许转载

本文链接: [https://blog.csdn.net/weixin\\_46081055/article/details/122378940](https://blog.csdn.net/weixin_46081055/article/details/122378940)

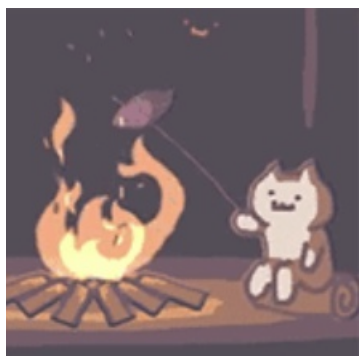
版权



[#EzOurCtf](#) [misc](#) 同时被 2 个专栏收录

7 篇文章 0 订阅

订阅专栏



[ctf](#)

81 篇文章 4 订阅

订阅专栏

## 2021长安“战疫”网络安全卫士守护赛 misc部分writeup

[八卦迷宫](#)

[朴实无华的取证](#)

[西安加油](#)

[ez\\_Encrypt](#)

一百多名, 我觉得还行欸, 多亏了队里的crypto手

### 八卦迷宫

签到题, 走迷宫, 换成字就可以了

### 朴实无华的取证

老规矩先看pslist

```
D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (D:\download\xp_sp3\xp_sp3.raw)
      PAE type : PAE
      DTB : 0x764000L
      KDBG : 0x8054e2e0L
      Number of Processors : 2
      Image Type (Service Pack) : 3
      KPCR for CPU 0 : 0xffdff000L
      KPCR for CPU 1 : 0xf8757000L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2021-12-27 02:37:41 UTC+0000
      Image local date and time : 2021-12-27 10:37:41 +0800

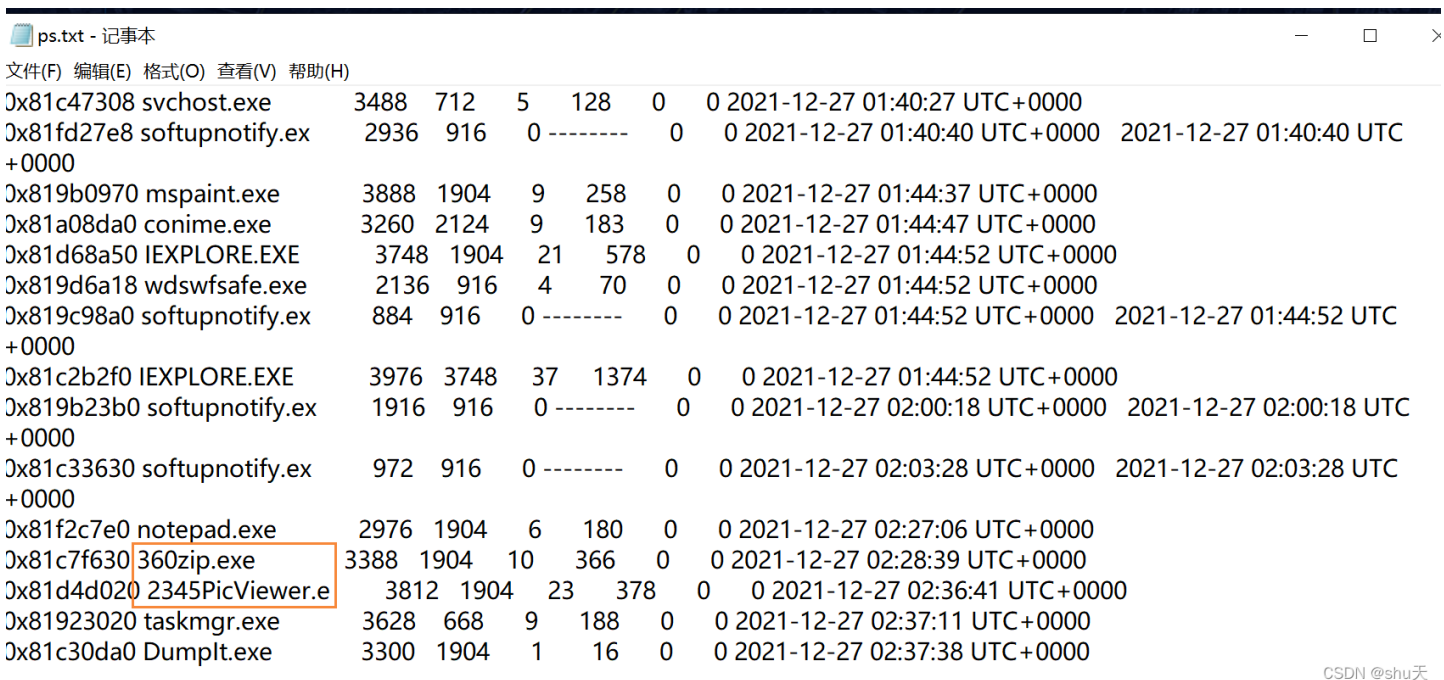
D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 pslist > 1\ps.txt
系统找不到指定的路径。

D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 pslist > 1\ps.txt
Volatility Foundation Volatility Framework 2.6

D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 filescan > 1\file.txt
Volatility Foundation Volatility Framework 2.6
```

CSDN @shu天

进程里面有 [文本查看器](#)，[360压缩](#)和[图片查看器](#)



```
ps.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
0x81c47308 svchost.exe      3488  712  5  128  0  0 2021-12-27 01:40:27 UTC+0000
0x81fd27e8 softupnotify.ex  2936  916  0  -----  0  0 2021-12-27 01:40:40 UTC+0000 2021-12-27 01:40:40 UTC
+0000
0x819b0970 mspaint.exe        3888  1904  9  258  0  0 2021-12-27 01:44:37 UTC+0000
0x81a08da0 conime.exe      3260  2124  9  183  0  0 2021-12-27 01:44:47 UTC+0000
0x81d68a50 IEXPLORE.EXE    3748  1904  21  578  0  0 2021-12-27 01:44:52 UTC+0000
0x819d6a18 wdswwfsafe.exe  2136  916  4  70  0  0 2021-12-27 01:44:52 UTC+0000
0x819c98a0 softupnotify.ex  884  916  0  -----  0  0 2021-12-27 01:44:52 UTC+0000 2021-12-27 01:44:52 UTC
+0000
0x81c2b2f0 IEXPLORE.EXE    3976  3748  37  1374  0  0 2021-12-27 01:44:52 UTC+0000
0x819b23b0 softupnotify.ex  1916  916  0  -----  0  0 2021-12-27 02:00:18 UTC+0000 2021-12-27 02:00:18 UTC
+0000
0x81c33630 softupnotify.ex  972  916  0  -----  0  0 2021-12-27 02:03:28 UTC+0000 2021-12-27 02:03:28 UTC
+0000
0x81f2c7e0 notepad.exe        2976  1904  6  180  0  0 2021-12-27 02:27:06 UTC+0000
0x81c7f630 360zip.exe          3388  1904  10  366  0  0 2021-12-27 02:28:39 UTC+0000
0x81d4d020 2345PicViewer.e    3812  1904  23  378  0  0 2021-12-27 02:36:41 UTC+0000
0x81923020 taskmgr.exe     3628  668  9  188  0  0 2021-12-27 02:37:11 UTC+0000
0x81c30da0 DumpIt.exe     3300  1904  1  16  0  0 2021-12-27 02:37:38 UTC+0000
```

CSDN @shu天

cmd运行过的程序也可以印证，发现有flag.zip和flag.png

```
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 cmdline
```

```

IEXPLORE.EXE pid: 3976
Command line : "C:\Program Files\Internet Explorer\IEXPLORE.EXE" SCODEF:3748 CREDAT:79873
*****
softupnotify.ex pid: 1916
*****
softupnotify.ex pid: 972
*****
notepad.exe pid: 2976
Command line : "C:\WINDOWS\system32\notepad.exe" C:\Documents and Settings\Administrator\姦明潰\鋤戩殞鏃 3 .txt.txt
*****
360zip.exe pid: 3388
Command line : "C:\Program Files\360\360zip\360zip.exe" "C:\Documents and Settings\Administrator\姦明潰\flag.zip"
*****
2345PicViewer.e pid: 3812
Command line : "C:\Program Files\2345Soft\2345Pic\2345PicViewer.exe" "C:\Documents and Settings\Administrator\姦明潰\flag.png"
*****
taskmgr.exe pid: 3628
Command line : taskmgr.exe
*****
DumpIt.exe pid: 3300
Command line : "D:\360淪文支嫻牠 鎧尤笈杞絀DumpIt\DumpIt.exe"

```

filesan取出flag.zip和flag.png

```

λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000
0000017ad6a8 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x017ad6a8 None \Device\HarddiskVolume1\Documents and Settings\Administrator\姦明潰\flag.z
ip
SharedCacheMap 0x017ad6a8 None \Device\HarddiskVolume1\Documents and Settings\Administrator\姦明潰\flag.zip

λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000
000001e65028 -D ./ -n
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x01e65028 None \Device\HarddiskVolume1\Documents and Settings\Administrator\姦明潰\flag.p
ng

```

flag.zip导出有损坏，可以winrar用自带的修复



密码是在记事本里面 20211209

```

D:\tool\qz\volatility\volatility_2.6_win64_standalone
λ volatility_2.6_win64_standalone.exe -f D:\download\xp_sp3\xp_sp3.raw --profile=WinXPSP2x86 notepad
Volatility Foundation Volatility Framework 2.6
Process: 2976
Text:
?

Text:
?↓

Text:
L

Text:
?

Text:
????????????????
20211209(encrypt)
????????????????????????????
????!?????
????!????

```

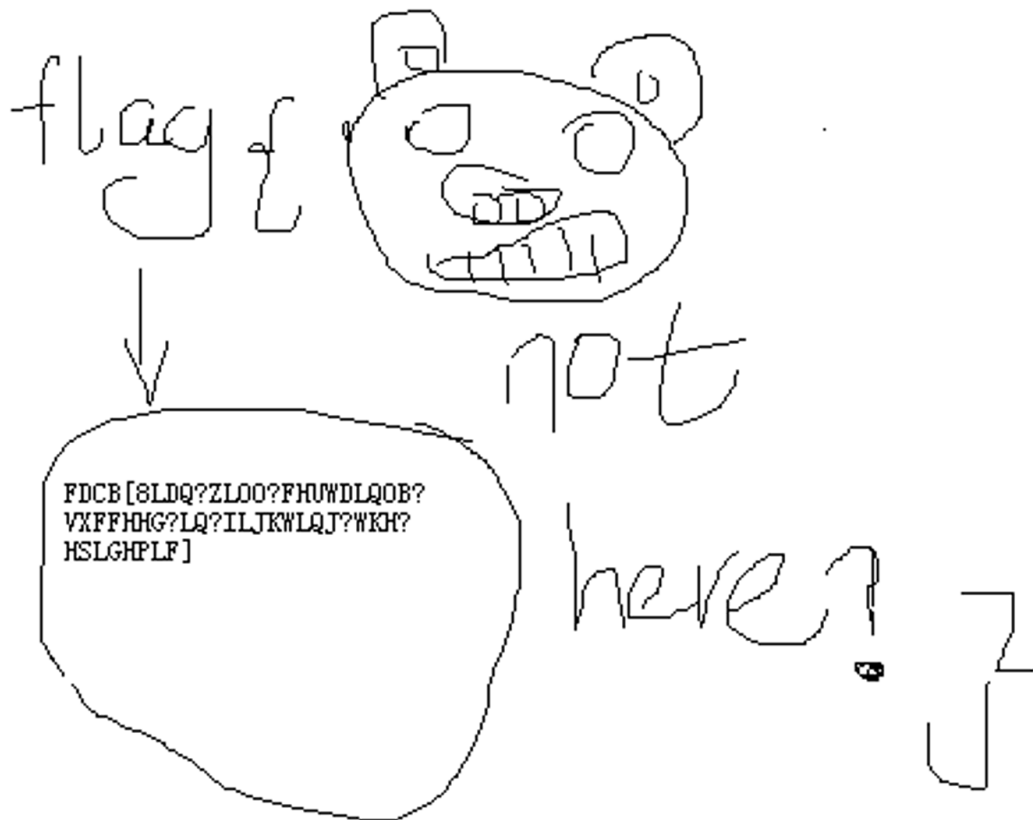
CSDN @shu天

encrypt.txt的内容

```

//幼儿园水平的加密（部分）
void Encrypt(string& str)
{
    for(int i = 0; i < str.length(); i++)
    {
        if(str[i] >='a' && str[i] <='w')
            str[i] += 3;
        else if(str[i] == 'x')
            str[i] = 'a';
        else if(str[i] == 'y')
            str[i] = 'b';
        else if(str[i] == 'z')
            str[i] = 'c';
        else if(str[i] == '_')
            str[i] = '|';
        str[i] -= 32;
    }
}

```



```
FDCB[8LDQ?ZLOO?FHUWDLQOB?VXFFHHG?LQ?ILJKWLQJ?WKH?HSLGHPLF]
```

解密脚本

```
e = "FDCB[8LDQ?ZLOO?FHUWDLQOB?VXFFHHG?LQ?ILJKWLQJ?WKH?HSLGHPLF]"
d = ""
for i in e:
    i = chr(ord(i)+32)
    if 'd'<=i<='z':
        i = chr(ord(i)-3)
    elif i=='a':
        i='x'
    elif i=='b':
        i='y'
    elif i=='c':
        i='z'
    elif i=='|':
        i=='_'
    d += i
print(d)
```

```
cazy{Xian_will_certainly_succeed_in_fighting_the_epidemic}
```

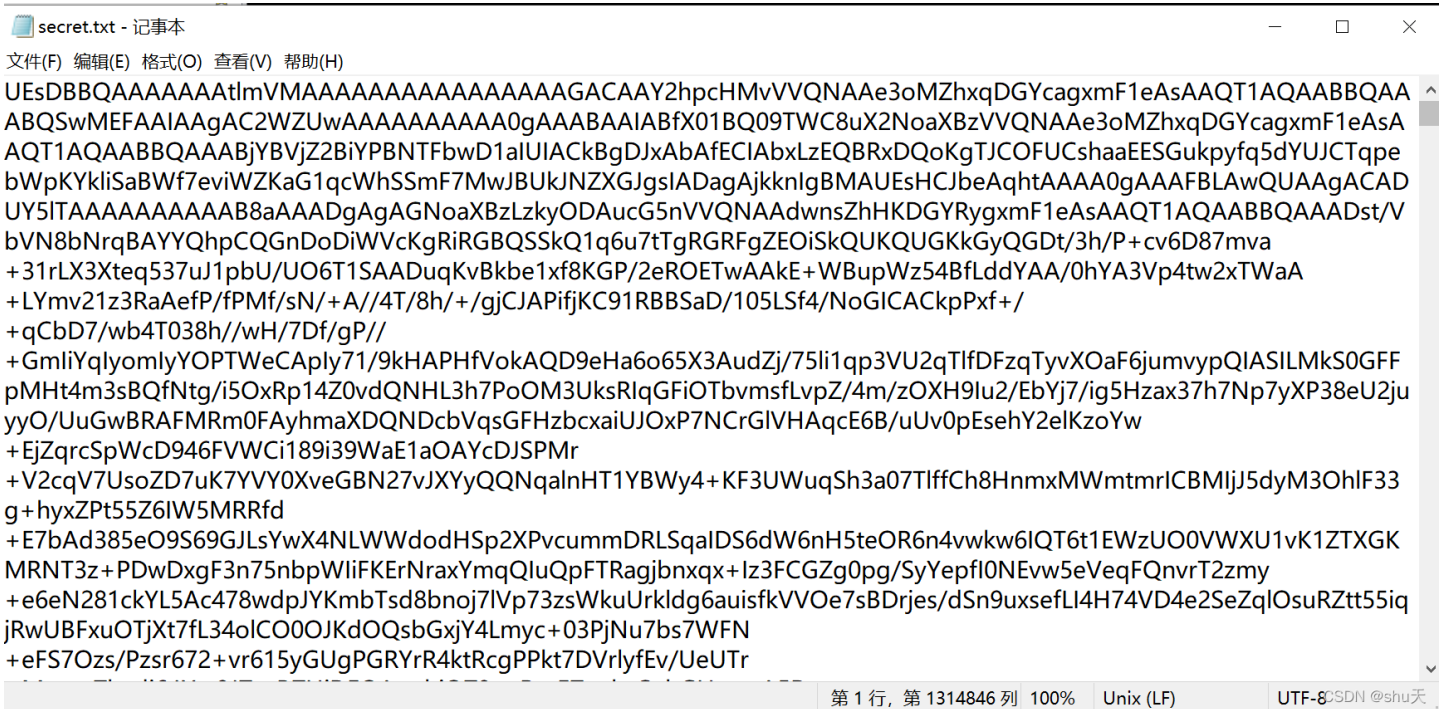
## 西安加油

发现http流里面有secret.txt





导出



base64解密 (<https://the-x.cn/base64>) , 发现是压缩包

## Base64 在线解码、编码

常规Base64

CSS Base64

DES加密/解密

3DES加密/解密

AES加密/解密

RSA加密/解密

```
UESDBBQAAAAAAtlmVMAAAAAAAAAAAAAAAAAAGACAAY2hpcHMvVQNA Ae3oMZhxdGYcagxmF1eAsAAQT1QAABBQAAABQSwMEFAAIAAgAC2WZUwAAAAAAAAAAAgAAABAAIABfX01BQ09TWC8uX2NoaXBzVQNA Ae3oMZhxdGYcagxmF1eAsAAQT1QAABBQAAABjYBvJ2BiYPBNTFbWd1alUIACkBgDjXAbAfECIAbxLzEQBRxDQoKgTJCOFUCshaaEESGukpyfq5dYUJCTqpebWpKYkIiSaBwF7eviWZKaG1qcWhSSmF7MwJBuKJNZXGJgsIADagAjkknlgBMAUESHCJbeAqhtAAAA0gAAAFBLAwQUAAGACADUY5ITAAAAAAAAAAB8aAADgAgAGNoaXBzLzkyODAUcG5nVQNAAdwnsZhHKDGYRygmF1eAsAAQT1QAABBQAAADst/VbVN8bNrqBAYYQhpCQGnDoDiWVcKgrIRGBQSSkQ1q6u7tTgRGRFgZE0iSkQUKQUGKkGyQGdt/3h/P+cv6D87mva+31rLX3Xteq537uJ1pbU/UO6T1SAADuqKvBkbe1xf8KGP/2eROETwAAkE+WBupWz54BfLddYAA/0hYA3Vp4tw2xTWaA+LYmv21z3RaAef/fPMf/sN/+A//4T/8h/+/gjCJAPifjK91RBBSaD/105LSf4/NoGICAcKpPxf+/+qCbD7/wb4T038h//wH/7Df/gP//+GmliYqlyomlyYOPTWeCAply71/9kHAPHfVokAQD9eHa6o65X3AudZj/75li1qp3VU2qTlfdFzqTyvXOaf6jumvypQIASILMkS0GFFpMhT4m3sBQfNtg/i5OxRp14Z0vdQNHL3h7PoOM3UksRlqGfIOTbvmsfLvpZ/4m/zOXH9lu2/EbYj7/ig5Hxaz37h7Np7yXP38eU2juyO/UuGwBRAFMrm0FAyhmaXDQNDcbVqsGFHzbcxaiUJOxP7NcrGIVHAqcE6B/uUv0pEsehY2elKzoYw+EjZqrcSpWcD946FVWCi189i39WaE1aOAYcdJSPMr+V2cqV7UsoZD7uK7YVY0XveGBN27vJXYQQNqalHT1YBWy4+KF3UWuqSh3a07TlffCh8HnmxMwmtmrICBMlj5dyM3OhIF33g+hYxZPt55Z6IW5MRRfd+E7bAd385e09S69GJLsYwX4NLWWdodHSp2XPvcummDRLSqaIDS6dW6nH5teOR6n4vwwk6lQT6t1EWzU00VWXU1vK1ZTXGKMRNT3z+PDwDxgF3n75nbpWlIFkErNraxYmqQluQpFTRagjbnqx+Iz3FCGZg0pg/SyYepfI0NEvw5eVeqFQnvrT2zmy+e6N281ckYL5Ac48wdpJYKmbTsd8bnoj7lVp73zswkuUrklDg6auisfkVVOe7sBDrjes/dSn9uxsefLI4H74VD4e2SeZqIosuRZtt55iqjRwUBFxuOTjXt7fL34olCO0JKdOQsbGxjY4Lmzc+03PjNu7WFWN+eFS0Zs/Pzsr672+vr615yGUgPGRYrR4ktRcgPPkt7DVrlyfEv/UEuTr
```

编码源格式:  文本  Hex 解码结果: 自动检测 中文编码: UTF-8

```
Zip Data Include:
-----
0Byte chips/
210Byte __MACOSX/._chips
26.12KByte chips/9280.png
172Byte __MACOSX/chips/._9280.png
15.07KByte chips/7125.png
172Byte __MACOSX/chips/._7125.png
```

```
24.24KByte    chips/7079.png
172Byte    __MACOSX/chips/._7079.png
27.78KByte    chips/5444.png
172Byte    __MACOSX/chips/._5444.png
28.13KByte    chips/9056.png
172Byte    __MACOSX/chips/._9056.png
23.33KByte    chips/3195.png
172Byte    __MACOSX/chips/._3195.png
17.41KByte    chips/7683.png
172Byte    __MACOSX/chips/._7683.png
27.06KByte    chips/4365.png
172Byte    __MACOSX/chips/._4365.png
10.00KByte    chips/.DS_Store
120Byte    __MACOSX/chips/._.DS_Store
21.25KByte    chips/7321.png
172Byte    __MACOSX/chips/._7321.png
17.42KByte    chips/1220.png
172Byte    __MACOSX/chips/._1220.png
```

插件【Zip】 Zip-based or zip file

另存为: zip文件

附加信息:

```
Encrypted:false
Files:100
Total Size:1182014
```

显示内容非原始信息

数据长度: 986,604 Bytes

插件数: 18, 耗时: 22ms

CSDN @shu天

里面是一堆图片，看起来是要拼图

montage和gap安装使用时参考的博客

[https://blog.csdn.net/m0\\_47643893/article/details/113778577](https://blog.csdn.net/m0_47643893/article/details/113778577)

<https://www.cnblogs.com/bhxdn/p/14094717.html>

<https://github.com/nemanja-m/gaps>

先把图片合成一张

```
sudo apt-get install montage
```

```
montage *.png -tile 8x6 -geometry +0+0 flag.png
```



然后用gaps拼图

```
gaps --image=./flag.png --size=100 --save
```





```

GET /public/web123 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
If-Modified-Since: Mon, 27 Dec 2021 06:30:20 GMT
If-None-Match: "12451a-5d41ad6b87e79"

```

```

HTTP/1.1 200 OK
Date: Mon, 27 Dec 2021 06:40:22 GMT
Server: Apache/2.4.48 (Debian)
Last-Modified: Mon, 27 Dec 2021 06:40:16 GMT
ETag: "124470-5d41afa47656c"
Accept-Ranges: bytes
Content-Length: 1197168
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

```

```

UESDBBQAAAAAAH0m1MAAAAAAEEEECAAYXBwL1VUDQAHFV/JVYhfyWFYX81hdXgLAEE
9QEAAAUAAAUEsDBBQACAAIAM0m1MAAAAAAANIIAAAOACAAX19NUNPU1gVL19hCBVVAOA
BlhfYWFYX81hb1/JYXV4CwABBPUBAAAEFAAAAGNGFWNnYgJg8E1MVvAPVohQgAKQGAMnEBSB8QI
BvEvMRAFHEHCgqBmkI4VQKyFpoQRIa6SnJ+r1lhQkJOq15takpiSWJJoFZ/t6+JZkpobWpxaFJKY
XszAkFsqk1lcYmCwgANqACOSSciaEwBQSwc1I4CgG0AAADSAAAAUEsDBBQACAAITANKokFMAAAAA
AAAAAAABAANCAAYXBwL2V2ZW50LnBocFVUDQA3Tm7Y1Y1TyWGNu81hdXgLAEE9QEAAAUAAA
s7EvyCjg0tdXeLKr+8nubU/XzXqys/PZtHYgm6sotaSOKE8hmksBCNSTMvNS1BXAwNYOKhirwWR
zMksLknNUOeRBEs4Fhr45mWwqEPEgerhMh41JQVBP4k4ZFzBlqHL+OSn+6SWpeaoY5MJL8osSUWR
gTuVuDsP0LkoMwkQZOMteYACFBLBwhGtdZWhQAAAAABAABQSwMEFAAIAAgAxHSbUwAAAAA
BCAAAA0AIBhcHAvLkRtXIN0b3JlVFNQAAADRX81h21vJYVffYWF1eAsAAQT1AAQABBBQAADTWTs

```

1 客户端 分组, 1 服务器 分组, 1 turn(s).

CSDN @shu天

再向上看，分析蚁剑命令执行的流量

The screenshot shows a Wireshark capture of an HTTP transaction. The top pane shows a list of 12 packets. The middle pane shows the details of the selected packet (No. 117), which is an application/x-www-form-urlencoded POST request to /public/shell.php. The bottom pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protcol	Length	Info
45	2021-12-27 14:39:51.01	activate.navicat...	activate.navicat.com	HTTP	4383	POST /public/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
47	2021-12-27 14:39:51.01	activate.navicat...	activate.navicat.com	HTTP	414	HTTP/1.1 200 OK (text/html)
57	2021-12-27 14:39:53.66	activate.navicat...	activate.navicat.com	HTTP	4416	POST /public/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
59	2021-12-27 14:39:53.66	activate.navicat...	activate.navicat.com	HTTP	442	HTTP/1.1 200 OK (text/html)
69	2021-12-27 14:40:01.51	activate.navicat...	activate.navicat.com	HTTP	4481	POST /public/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
71	2021-12-27 14:40:01.52	activate.navicat...	activate.navicat.com	HTTP	416	HTTP/1.1 200 OK (text/html)
81	2021-12-27 14:40:06.41	activate.navicat...	activate.navicat.com	HTTP	4412	POST /public/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
83	2021-12-27 14:40:06.42	activate.navicat...	activate.navicat.com	HTTP	294	HTTP/1.1 200 OK (text/html)
93	2021-12-27 14:40:07.01	activate.navicat...	activate.navicat.com	HTTP	280	GET /wpad.dat HTTP/1.1
95	2021-12-27 14:40:07.01	activate.navicat...	activate.navicat.com	HTTP	539	HTTP/1.1 404 Not Found (text/html)
105	2021-12-27 14:40:07.32	activate.navicat...	activate.navicat.com	HTTP	4410	POST /public/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
107	2021-12-27 14:40:07.33	activate.navicat...	activate.navicat.com	HTTP	425	HTTP/1.1 200 OK (text/html)
117	2021-12-27 14:40:16.61	activate.navicat...	activate.navicat.com	HTTP	4477	POST /public/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
119	2021-12-27 14:40:16.77	activate.navicat...	activate.navicat.com	HTTP	295	HTTP/1.1 200 OK (text/html)
129	2021-12-27 14:40:22.24	activate.navicat...	activate.navicat.com	HTTP	642	GET /public/web123 HTTP/1.1
292	2021-12-27 14:40:22.28	activate.navicat...	activate.navicat.com	HTTP	2131	HTTP/1.1 200 OK

**Hypertext Transfer Protocol**

- POST /public/shell.php HTTP/1.1\r\n
- Host: localhost\r\n
- Accept-Encoding: gzip, deflate\r\n
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_7\_3) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.3 Safari/534.53.10\r\n
- Content-Type: application/x-www-form-urlencoded\r\n
- Content-Length: 4115\r\n
- Connection: close\r\n
- \r\n
- [Full request URI: http://localhost/public/shell.php]
- [HTTP request 1/1]
- [Response in frame: 119]
- File Data: 4115 bytes

**HTML Form URL Encoded: application/x-www-form-urlencoded**

- Form item: "cazy" = "@ini\_set('display\_errors', '0');@set\_time\_limit(0);function asenc(\$out){return \$out;};function asoutput(){@output=ob\_get\_contents();@ob\_end\_clean();echo "ba\$"."322";echo @asenc(\$output);echo "6fd"
- Form item: "fe52cc8ae5662a" = "EEL2pbib9zaa=="
- Form item: "w844661a730e14" = "gy"
- Form item: "zafcd0a3b9be19" = "K2y2ogIi92YIVd3d3L2h0bWwvHvib1JiYXNlNjQgd3d3LnppcCA+IHdlYyEymZtlYzhvIFRtXTtw2QzWmobyBbRV0="

0160 20 63 6c 6f 73 65 0d 0a 0d 0a 63 61 7a 79 3d 25 close...cazy%  
0170 34 30 69 6e 69 5f 73 65 74 28 25 32 32 64 69 73 40ini\_se...%2d01%  
0180 70 6c 61 79 5f 65 72 72 6f 72 73 25 32 32 25 32 play\_err...ors%22%  
0190 43 25 32 30 25 32 32 30 25 32 32 29 25 33 42 25 %2d%20%22%32%3B%  
01a0 34 30 73 65 74 5f 74 69 6d 65 5f 6c 69 6d 69 74 40set\_t...ime\_limit%  
01b0 20 30 29 25 33 42 66 75 6e 63 74 69 6f 6e 25 32 0%2836fu...nction%  
01c0 33 61 73 69 6e 63 28 25 33 34 6f 39 74 39 33 37 @asenc(%...\$out)%3B%  
01d0 42 72 65 74 75 72 6e 25 32 30 25 32 34 6f 75 74 @return%...28%24out%  
01e0 25 33 42 25 37 44 25 33 42 66 75 6e 63 74 69 6f 33%37%03...Bfunction%  
01f0 6e 25 32 30 61 73 6f 75 74 70 75 74 28 29 25 37 %2d%asou...tput(%3B%  
0200 42 25 32 34 6f 75 74 70 75 74 25 33 44 6f 62 5f %2d%outp...ut%3Dob%  
0210 67 65 74 5f 63 6f 6e 74 65 6e 74 73 28 29 25 33 @et\_con...ents(%3B%  
0220 42 6f 62 5f 65 6e 64 5f 63 6c 65 61 6e 28 29 25 @ob\_end...\_clean(%3B%  
0230 33 42 65 63 68 6f 25 32 30 25 32 62 61 35 25 3eBecho%...2%2ba%3B%  
0240 32 32 2e 25 32 32 31 32 32 25 32 25 33 42 65 72.%22%32...2%23%3B%  
0250 63 68 6f 25 32 30 25 34 30 61 73 65 6e 63 28 25 %2d%2d%...@asenc%4

CSDN @shu天

```
cd "/var/www/html/public";base64 www.zip > web123;echo [S];pwd;echo [E]
```

是吧www.zip的备份base编码成web123了

### Base64 Encoding

Encode Decode  

Pattern  
Base64

```
Y2QgIi92YXlvd3d3L2h0bWwvcHVibGljitiYXNINjQgd3d3Lnp  
pcCA+IHdlYjEyMztlY2hvlFtTtXtd2Q7ZWNoYBbRV0=
```

```
cd "/var/www/html/public";base64 www.zip > web123;echo  
[S];pwd;echo [E]
```

CSDN @shu天

转成zip

```
WyINAAAAAXAAAAAQIAIAAAAAAAAAAAKSB6fELAHZlBmRvci90b3B0aGluay9mcmFtZXdvcm5vc3Jj  
L3RoaW5rL2NvbnNvbGUvY29tbWFuZC9tYWtlL3N0dWJzL2NvbnRyb2xsZXlucGxhaW4uc3R1YlVU  
DQAHAeX4YjTtYWGbu8lhdXgLAEE9QEAAAQUAAAAUESBAHQDFAAAAAAAE6bUwAAAAAAAAAAAAAA  
AAUAIAAAAAAAAAAAAAO1B2PILAHZpZXcvVVQNAAEU8lhtlPJYRNWYWF1eAsAAQT1AQAABBQAAABQ  
SwECFAMUAAgACAAQbptTt4CqG0AAADSAAAADwAgAAAAAAAAAAAAA7YEB8wsAX19NQUNPU1gvLI92  
aWV3VVQNAAEU8lhtlPJYWF9fyWF1eAsAAQT1AQAABBQAAABQSwECFAMUAAgACADSqJBTct5pUzIA  
AAAtAAADgAgAAAAAAAAAAAAApIH8wsAdmldy9SRUFETUuubWRVVA0AB905u2GSU8lhkIPJYXV4  
CwABBUBAAAEEFAAAAFBLBQYAAAAOAM4Az2RAQBz9AsAAAA=
```

编码源格式:  文本  Hex 解码结果: 自动检测 中文编码: UTF-8 编码 解码

Zip Data Include:

```
0Byte app/  
210Byte __MACOSX/._app  
256Byte app/event.php  
8.00KByte app/.DS_Store  
120Byte __MACOSX/app/._.DS_Store  
266Byte app/AppService.php  
137Byte app/service.php  
0Byte app/controller/  
210Byte __MACOSX/app/._controller  
1.37KByte app/ExceptionHandle.php
```

插件【Zip】 Zip-based or zip file  
另存为: zip文件  
附加信息:  
Encrypted:false  
Files:824  
Total Size:2576753

显示内容非原始信息  
数据长度: 886,214 Bytes  
插件数: 18, 耗时: 26ms

CSDN @shu天

然后比赛时候我就卡住了，其实联系题目里的Encrypt，可以猜想是用了什么加密函数。  
D盾扫描一下就找到了

扫描结束 扫描结束. 检测文件数:569 发现可疑文件:1 用时:1.38秒 返回

文件 (支持拖放目录和扫描)	级别	说明	大小	修改时间
d:\download\from_the_x\app\controller\index.php	4	加密文件	5212	2021-12-27 13:59:42

CSDN @shu天

```
# \app\controller\index.php
<?php define('IK1Sux1227', __FILE__); $DusPFr=base64_decode("bjF6Yi9tYTVcdnQwaTI4LXB4dXF5KjZscmtkZz1fZWhjc3dvNctmM
zdqZHF0d31pT2VBY1VaTHBDdUhuYm1ndkZzZlNhUf1sTUpCTmpSvmtLeFFeVfDjcnpFb1hHaA=="); $arCiCL=$DusPFr[3].$DusPFr[6].$Dus
PFr[33].$DusPFr[30]; $VvUrBZ=$DusPFr[33].$DusPFr[10].$DusPFr[24].$DusPFr[10].$DusPFr[24]; $DEomKk=$VvUrBZ[0].$DusP
Fr[18].$DusPFr[3].$VvUrBZ[0].$VvUrBZ[1].$DusPFr[24]; $LnPNvY=$DusPFr[7].$DusPFr[13]; $arCiCL.= $DusPFr[22].$DusPFr[
36].$DusPFr[29].$DusPFr[26].$DusPFr[30].$DusPFr[32].$DusPFr[35].$DusPFr[26].$DusPFr[30]; eval($arCiCL("JFZDQ1pRVz
0iZ29NVFFoZXFpYVVPdWjTWZSS1Nya1d0bmrFc1BaR2pBS3BDVnRCSuH3REZ4Y3pTYGx2eVlUY21VdVBuZ3BzeXfIb09saGpGSVpOU3d6bU1IR3
ZEeHRRWFZhv2ZkQUpFc1JLTENCUWVISj1BcGR4WUd2Vm9wTjVcDfH6WmhCdXVwWmZyY0RmM2p1cmpGMnJpekXZcmNEZjN0aU1aR21qbmkwOWpITm
p1UjJzZM1NF0VpHT1NRR3ZzVGZvam5oREdHcGlCME5WaE5PMmhxc0x6dVZtWjBpRXVYU3ZoT2hEVkNwQmtLTzIxMHAxazZidkdwVjJ1bk9LU1p6Wj
VKenYxU1BvaHJPMXo0ekV6cWlEVkdjMUdVvNyxQXmXU3ZVWjVzRkVrVFZaV1iVkvMVR0VqRGJCZktWmHVBEk5tQXpkEKZoVmtrc05ycGIxek9wRw
hwVktCd1ZEV1podkVMc0JHaUdLMD1mZ1o3am1rM2JadTFWSzBaR21qbmkwOWpOS1N6Q2dow1Vva0hpMEJiU0IwcWp2aFhwWj1IR1ZNS2MxMHFqdm
hYcFo5SEZWTUtjRTA3amRHaG12emRGSzBaR21qbmkwOWpOS2NLTEY0Wkdtam5pMD1qTktTQUxGNFPbHbWpuaTA5ak5LzjBMRjRaR21qbmkwOWpOS2
1BTEY0Wkdtam5pMD1qTktTMEExpTvPOTkdNendHc0hGaDjzc3J3aDBhYmNFMHFqdmhYcFo5SEZWTXJ5RTBxanZoWHB0aUhgVkl1TEY0WnpCRWNHMH
pDTktXekNnaDjzc3J3aDBhYmNWMHFqdmhYcFo5SEZWTWTRTA3anYxRVVWRXZPSzBaR21qbmkwOWpOS3p6Q2dow1Vva0hpMEJiY21Ten1laHR6Mj
Vme1ZScUhGaFpVb2tIaTBCYmNEanpDZ2haVW9rSGkwQmJjS0d6Q2dow1Vva0hpMEJiY0RCekNnaFpVb2tIaTBCYmNER3pDZ2haVW9rSGkwQmJjS1
d6Q2dow1Vva0hpMEJiY0tqekNnaFpVb2tIaTBCYmNlVnpDZ2haVW9rSGkwQmJjREd6Q2dow1Vva0hpMEJiY0tXenkyVjJPTkFUam1rM2JadTFWZV
1nR1pWcG1VWHJSGZtOcERXa1ZfVjBSQ1R1U0xoc2h0ck1zTnJwcEJqT05vQ1poTmhFR05hVE9WR05HbWpaVjFUS1YwenZTVmphUEVWREZtNTVOWn
pBaHZmZXBFA1Zjb3JpczJyTVNFVUtoWj1WaFZqS1Z2NU16V1RBekVXZ2h0dUZPS2pwcZFaS05CekJidmhTVlpweXBWQk5SS1dwV5yTk9EV05oMV
ZkYkVoZ1ZOVUtWRXVYUHZWZHNcQ1pWb3J1czIxQVB0RUvOWmpCcG9yTVZCVjRwd1ZWaEJ1eWhkV2tpS2p0Y0JCTHoyOXRQRf1JRndaMHAxU3FHZF
ZpRkVHT0YU0zJq1ZlWUHY1RmNku1FGWkdNYk5qZk5Eak5VMnpJc29hNGJCenFpQnpjVTFqMHNCVnZzQmpaUxTdGhLRXZzVkd2aDFCNxAzU3Rob3JhT1p1cGNCR0pHMmFGcDN1cVYyNXlWMHJtVUxTdGhLRXZzVk
d2aDFCNxAzV0Nzmk0zZmdaa3lLOctISj1BcGR4WUd2Vm9wTjVcDfH6ZEdu3RicZryY0RmM2p1cmpGMnJpekXZcmNEZjN0aU1aaEJrUVBtajBITm
p1UjJzZM1NF0VpHT1NRR3ZzVGZvam5oREdHcGlCME5WaE5PMmhxc0x6dVZtWjBpRXVYU3ZoT2hEVkNwQmtLTzIxMHAxazZidkdwVjJ1bk9LU1p6Wj
VKenYxU1BvaHJHc1ZaVnZtZVMekRiRVQyT0tFRk52aGFwWmhWym1HME90MVR0TKVPYkVfWmNoc1VzS1dGekJFSWjtyU5WMEduc1ZzMXBwa1ZwZF
NwRm1HdXNVUzjVmhkTm81c3NpMD1mZ1o3anYxVYydWlGSjBaaEJrUVBtajBOS1N6Q2dodk5v0TRVd2hiU0IwcWpT3BiM3VYekVNS2MxMHFqbU
dwYjN1WHpFTUtjRTA3akVHR1YyUzRHSjBaaEJrUVBtajBOS2NLTEY0WmhCa1FQbWOWtktTQUxGNFPoQmtRUG1qME5LzjBMRjRaaEJrUVBtajBOS2
1BTEY0WmhCa1FQbWOWtktTMEExpTvPPTkdWekJ6c0hGaE50VnpEUHZoYmNFMHFqbUdwYjN1WHpFTXJ5RTBxam1HcGIzdVh6RU1LTEY0WlZCQkxPM3
VaTktXekNnaE50VnpEUHZoYmNWMHFqbUdwYjN1WHpFTWTRTA3anZCwnoyc1NzSzBaaEJrUVBtajBOS3p6Q2dodk5v0TRVd2hiY21Ten1laGFiqn
pUczBZcUhGaHZ0bzk0VXdoYmNEanpDZ2h2Tm85NFV3aGjS0d6Q2dodk5v0TRVd2hiY0RCekNnaHZ0bzk0VXdoYmNER3pDZ2h2Tm85NFV3aGjS1
d6Q2dodk5v0TRVd2hiY0tqekNnaHZ0bzk0VXdoYmNlVnpDZ2h2Tm85NFV3aGjJREd6Q2dodk5v0TRVd2hiY0tXenkyVjJPTkFUanYxcVYydWlGWF
1nR1p6cHMxVnFzRGhHUERXa1ZOYTRpMmhJY21oQmJ0dW5zWlZwz3ZoRUZCekZjc0d1czF1WnpWa2RjTEJnaEJqTnNpVzBob0VMR3YxQ1ZvcnJWaV
N5UEVFTlVaYVp0bWprczB6TnBFenZHZGpnYzFmMXMxek1S1Q1pyaW81R1ZzRzRPREVGT1ZWRUd2ckZWTGhKvM1zcnMyU2RTVmp0Y0JR53NaR01oRW
hJTndrWmNEBTJWMEdY0JTZFJ2Qk50RU8wczI1dHN2RWRzRGoPvNzYsnMyNU5Wmmp2VkJTRFZCanZPMmFNVTJjQX1za2dw2hmTzFwdHB2U0xpRF
NOVm1acm1zenZzMD1PukVHRmNzamarPRFf0cDjQRWNMqM1WS1ZjC0RTd1UxQk9ob2twYl01NXMxUjFibTFUyMRFc05FR2pPvkDORkVaZVN0dVpjM1
dLTm9ydeZVnFpd0JpVlo1Y3NaUjFsvmpWR0VfEwhMaGZwC2hGaUJmc1V3RUZORUd1c21qTnMyU05pWkd0Y3ZyQVZCVjRjRwPvNvKxCR2MzV3ZPMm
EwUjJWRUZvYWhjZGhhVm9heXB2aE5VQmtOVk5oMudKVzBGRWpzaEJHVnAyYTNzmk00U05FSXptdWdiTFd2c0RFV2N2amR0bz1naExoYVzVYXlpdm
hPUMRTaWNCa0xzaVcwY1ZHSW1acnBiZfDrc0JHTWhVFEFWQ1dTVnNreUdFe1RwMVNmaG1Wk5FamhHbUdORnMwc1JkV0dWmWt5Vkv6Nhp2am5Hdj
FMVkJrbXNlanBWMW1BenYxTnAwNwN0b3JwaEVjS1ZCRXV1c1Y1VnNwEYxVUtoRedpYlpra09vMTRGRVnkr3Z1U2J2UzVzMXVFU05FRVZCV21WmN
J2c0RFWnAxU2ZoaVZaTkVqaEdtR05GczByUmRXR1Yxa3lWRXo0enZFbUd2MuxWQmttct0tqcFYxbUF6djF0cDA1SE5CekZoRWN1Tkj6aGNkaGFwB2
F5aXZoVnBkVnNORUdoc29yTk5CR01iRUVTYm1mMk8za2pTvkdFemR1WmgycmNzWlZNT1ZVZVNOcnBjZGg0TkRqdEzZMXFod0VpY0VqdE9WR05zRU
9BaUJqU3BCanFzS1NaU29qRXp2MU5wMDVjR0VofIXa01iRXpoY2RoYVYyYXRpQ1VBCpEpaXBLQmVzaVd0aVZwZfJka1NjMwprVkJoaMNFbWVWQm
haaEVUMFZEajBVMUdOaFprWmJFR3BzaWp0Y1Z6Tk5aaG1jQmt1aURqcE5CR01pWnJwYkVrbXNlanBWMW11aEJTVmhtan1PMmFUU1ZjZU5aNVpjMD
U1Tk5rT1NtMU5S5bXJOYzBzMVYwVkfzb2h2c3dqVmh2dw50VmhFU1ZzZXptak5wMgt1c1ZHQWkyRTZGd3VWtnZ1NU9va05Td1NhU0pFQkZtazFpQn
VUUE5qbmJtQ1ZjM1dLc0tqcFYxbUF6SkvTAdN1SE5CEmh5c0JuenZyWmJzR0tGMFNEQzFXa08zVnRoS0UxVkrRqVFZFU0pHMmFOYnZyT05pU1RwMG
FKc291cGJFT2VWREVOyJBrZE5CU1ZiQmYwTkkCM3AyRUxzRFNnaGlFc0Yya2pSbXJKc291cGJFT2VWREVOyJBrZE5CU1ZiQmYwTkkCM3AyRUxzRF
NnaGlFc21tU0ZSRWtmR2RTc1ZaMUFpbVNGcEVrTVZEak5jVkvRR1p6cHMxVnFzRGhHUEx6M21tU0ZSRWtmR2RTc1ZaMUFGMVnJUm05M0hpMGd0R1
o3SEs0PSI7ZXZhbCgnPz4nLiRhckNpQ0woJFZ2VXJCWigkREVvbuTrKCRWQ0JaUvcsJEXucG52WsoyKSwkREVvbuTrKCRWQ0JaUvcsJEXucG52WS
wkTG5wbnZKSwkREVvbuTrKCRWQ0JaUvcsMCwkTG5wbnZKSkpKts=")); ?>
```

## PHP混淆类在线破解（非组件类加密\*ZEND类加密请使用《PHP找源码VIP版》,免费版）

Zend Guard 6 加密的 Php 5.4/5.5/5.6全球首破,可以帮助您找回丢失的代码.有需要的请联系QQ:7530782  
本系统仅以测试为目的,是为了方便源码作者找回丢失的源码,不得用于商业用途。

现支持: **phpjm**、**phpd神盾**、**php微盾(威盾)**、**tianyiw**、**小猪**、**齐博**等各类混淆加密。(支持未知混淆破解)

PHP混淆加密在线还原 (\*加密程序容易,破解程序不容易.且行且珍惜!各路大神高抬贵手, 拜谢!)解不了的文件加QQ 7530782!

PHP加密文件:	<input type="text" value="选择文件"/> Index.php	*(请保持原文件名称(文件名不要有中文), 原版PHP文件请不要修改!)
文件编码:	<input checked="" type="radio"/> UTF-8 <input type="radio"/> GBK/GB2312	*这么牛的工具, 你的小伙伴都惊呆了, 还不快点告诉他们?!
解密选项:	<input type="checkbox"/> 格式化美化代码 <input checked="" type="checkbox"/> 清理代码(如果解密不正常, 请取消此选项) <input type="checkbox"/> 编码修复(&#、\x、\u、%u、chr)类修复(更强大修复请用:PHP代码修复) <input checked="" type="checkbox"/> 修复dirname乱码	
验证码:	<input type="text" value="4581"/>	*如果这个工具无法解密,请使用VIP版本,感谢您的支持!
<input type="button" value="解密PHP混淆文件"/>		

CSDN @shu天

```
Index.php  Index (2).php x
use app\BaseController;↓
↓
class Index extends BaseController↓
{↓
    public function index()↓
    {↓
        if(!empty($_GET['pop']))↓
            unserialize(base64_decode($_GET['pop']));↓
        }↓
        return "Welcom To CAZT! Xi'an Come On!";↓
    }↓
↓
    public function C4zyC0m3On()↓
    {↓
        return 'cazy{PHP_ji4m1_1s_s00000_3aSyyyyyyyyyy}';↓
    }↓
}↓
?>←
```

CSDN @shu天

得到flag 'cazy{PHP\_ji4m1\_1s\_s00000\_3aSyyyyyyyyyy}'